Advances in Mathematics **138**, 306–322 (1998)
Article No. AI981750

Mutually Isospectral Riemann Surfaces

Robert Brooks

Department of Mathematics, Technion–Israel Institute of Technology, Haifa, Israel

and

Ruth Gornet and William H. Gustafson

Department of Mathematics, Texas Tech University, Lubbock, Texas 79409-1042

Received March 27, 1997; accepted March 2, 1998

In this paper, we address the following question: Given a natural number

It was shown by Buser in [Bu] that there is an upper bound $N(g)$ to the size of such isospectral sets, depending only on the genus. More precisely, he gave the following upper estimate for $N(g)$:

THEOREM 0.1 ([Bu]). $N(g) \leqslant e^{720g^2}$.

The problem of finding a lower bound for $N(g)$ was addressed by R. Tse in [Tse1, 2], where he showed that:

THEOREM 0.2 ([Tse1, 2]). *There exists a sequence $g_i \to \infty$ and a constant c such that*

$$N(g_i) \geqslant c\sqrt{g_i}.$$

In this paper, we will exhibit a constant c and a sequence $g_i \to \infty$ such that

$$N(g_i) \geqslant g_i^{c \cdot \log(g_i)}.$$

In particular, the number of isospectral, nonisometric Riemann surfaces of genus g grows faster than polynomially in g. Our construction will give a value of c of approximately $1/(4\log(2))$.

More precisely, we have:

THEOREM 0.3. *For each natural number $n > 2$ and prime p, the number $N(g)$ of mutually isospectral Riemann surfaces of genus*

$$g = 1 + (n-1)\, p^{2n}$$

0001-8708/98 $25.00

is at least

$$N(g) \geqslant p^{(n^2-n)}.$$

For $n=2$, *we have* $N(g) \geqslant p^2$ *for* $g = 1 + 2p^4$.

To give some specific numerical examples, we construct 4096 mutually isospectral surfaces of genus 769, and over a billion mutually isospectral surfaces of genus 20,481. The first examples of isospectral pairs of surfaces were found by Vignéras in [Vig1, 2], and had genus 201,601. By contrast, for the somewhat smaller genus of 98,304, we find over 4 trillion surfaces all of which are isospectral to each other.

The idea behind our proof may be described as follows: In [GW] Gordon and Wilson exhibited continuous families of isospectral nilmanifolds, by constructing almost-inner deformations of 2-step nilpotent Lie groups. See [DG] for a thorough development of this point of view. At about the same time, Sunada [Su] gave a recipe for constructing isospectral manifolds via finite group theory.

We will combine these two approaches in the following way: We will in effect construct finite-group analogues of the Gordon–Wilson deformations, to which the Sunada construction will apply. The analogue of continuous families of isospectral manifolds then will be large finite sets of mutually isospectral surfaces.

We will also consider analogous problems in the setting of graphs and of number fields. We will show:

THEOREM 0.4. *For any* n, *there are* 2^{n-1} *isopectral graphs that are* 6*-regular with* $4n$ *vertices.*

The construction here uses the technique of Seidel switching, see [CDGT] for a discussion. There is no known method to yield corresponding isospectral manifolds from these isospectral graphs. See [BL] for a discussion.

THEOREM 0.5. *For all natural numbers* n *and odd primes* p, *there exist*

$$N(d) = p^{n^2-n}$$

nonisomorphic number fields of degree

$$d = p^{2n}$$

over the rational numbers that have the same zeta function.

1. MUTUALLY ISOSPECTRAL GRAPHS

In this section, we will show:

THEOREM 1.1. *For every k, there is a family of distinct 6-regular graphs $G_1, ..., G_{j_k}$, with the following properties*:

(a) *$G_1, ..., G_{j_k}$ all have $4k$ vertices.*

(b) *$G_1, ..., G_{j_k}$ are all isospectral.*

(c) *$j_k = 2^{k-1}$.*

The basis of our construction is the following lemma, which is a variant of the construction of Seidel Switching (see [CDGT], see also [BL]):

LEMMA 1.1. *Let $\{C_i\}_{i \in I}$ be a collection of graphs, and, for each unordered pair (i, j), $i \neq j$, let $P(i, j)$ be a collection of edges joining vertices of C_i with vertices of C_j, with the following properties*:

(a) *Each C_i is k-regular for some k.*

(b) *For each pair (i, j), either $P(i, j)$ is empty or, for each $v \in C_i$, v is joined by an element of $P(i, j)$ to exactly half the vertices of C_j, and, conversely, for each $v \in C_j$, v is joined by an elements of $P(i, j)$ to exactly half the vertices of C_i.*

Let $f: I \to \{0, 1\}$ be a partition of $\{C_i\}$ into two sets I^0 and I^1. Denote by Γ the graph whose vertices are the union of the vertices of the C_i's, and whose edges are given by:

(a) *If v and w both lie in C_i, then the set of edges joining v to w are the edges in C_i joining v to w.*

(b) *If v lies in C_i and w lies in C_j, $j \neq i$, then v is joined by an edge to w in Γ if and only if the edge (v, w) lies in $P(i, j)$.*

Let Γ^f denote the graph whose vertices are the same as Γ, but whose edges are described as follows:

(a) *If v and w both lie in C_i, then the set of edges joining v to w are the edges in C_i joining v to w.*

(b) *If v lies in C_i, w lies in C_j, and C_i and C_j both lie in I^0 or I^1, then v is joined to w in Γ^f if and only if the edge (v, w) lies in $P(i, j)$.*

(c) *If v lies in C_i, w lies in C_j, and one of C_i and C_j lies in I^0 while the other lies in I^1, and if $P(i, j)$ is non-empty, then v is joined by an edge to w in Γ^f if and only if the edge (v, w)* does not *lie in $P(i, j)$.*

Then Γ and Γ^f are isospectral.

Before proceeding with the proof of Lemma 1.1, we will take a simple case of the lemma. This case will serve as an illustration of the lemma, but will also serve as a building-block for our later construction.

We will consider the graphs C_1 and C_2 to both be the 2-regular graph C which is the disjoint union of a loop and a circle of length 3, as shown in Figure 1 below. The collection of edges $P(1, 2)$ is as shown in Figure 2. We will choose $f(1) = 0$ and $f(2) = 1$. Then Γ is as shown in Figure 3 below, and Γ^f is as shown in Figure 4 below.

Note the following properties of Γ and Γ^f: first of all, one of them (Γ^f) is a planar graph, while the other (Γ) is not planar. Secondly, Γ contains two loops joined by an edge, while Γ^f does not.

We now turn to the proof of Lemma 1.1.

Let γ be a closed path in Γ, and let n be the length of γ. Let $v_0, ..., v_{n-1}$ be an indexing (mod n) of the vertices along γ, so that v_i is joined to v_{i+1} by an edge of γ. Let I^0 denote the set containing the C_i which contains v_0.

Let $C^\Gamma(\gamma)$ (resp. $C^{\Gamma^f}(\gamma)$) denote the class of closed indexed paths in Γ (resp. Γ^f) with the following property: The path γ' with indexing $v'_0, ..., v'_{n-1}$ lies in $C^\Gamma(\gamma)$ (resp. $C^{\Gamma^f}(\gamma)$) if and only if:

(a) If $v_i \in I^0$, then $v'_i = v_i$.

(b) In all cases, v_i and v'_i lie in the same C_j.

If we can show that the cardinality of $C^\Gamma(\gamma)$ equals the cardinality of $C^{\Gamma^f}(\gamma)$ for all choices of γ, then we shall have shown that Γ is isospectral to Γ^f, since we will have constructed a bijection of paths of length n in Γ to paths of length n in Γ^f, for all n.

FIG. 1. The graph C.

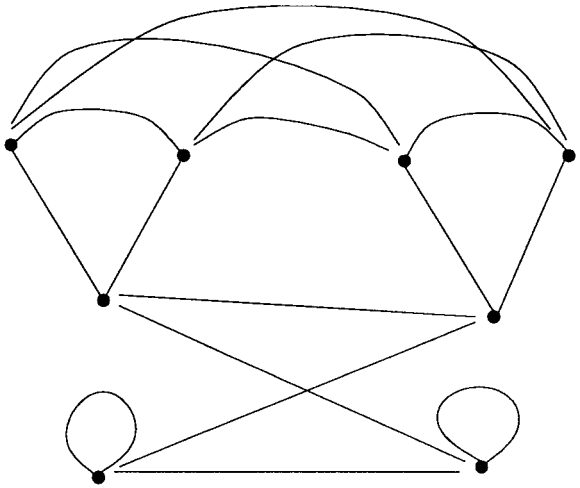

FIG. 2. The edges $P(1, 2)$.

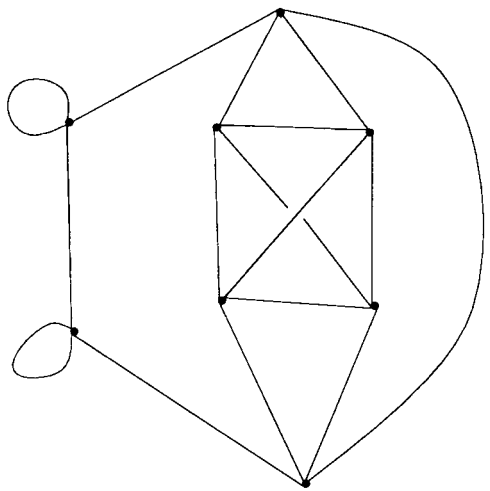

FIG. 3. The graph Γ.

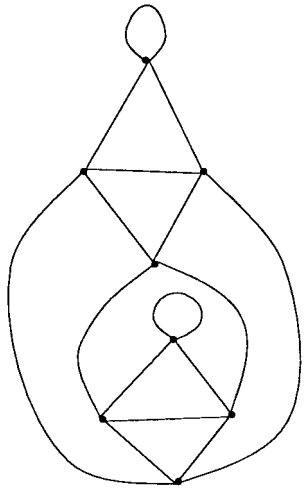

FIG. 4. The graph Γ^f.

But let i be an index such that v_i lies in I^0, but v_{i+1} does not, and let k be such that the next vertex lying in I^0 is v_{i+k}. Let W_i^Γ denote the set of all paths $(w_1, ..., w_{k-1})$ such that w_j and v_{i+j} lie in the same C_l.

We will partition W_i^Γ into four sets:

$$W_i^\Gamma(0,0) = \{(w_1, ..., w_{k-1}) : w_1 \text{ is joined by an edge in } P(i,j) \text{ to } v_i, \text{ and } w_{k-1} \text{ is joined by an edge to } v_{i+k}.\}$$

$$W_i^\Gamma(0,1) = \{(w_1, ..., w_{k-1}) : w_1 \text{ is joined by an edge in } P(i,j) \text{ to } v_i, \text{ and } w_{k-1} \text{ is not joined by an edge in } P(i,j) \text{ to } v_{i+k}.\}$$

$$W_i^\Gamma(1,0) = \{(w_1, ..., w_{k-1}) : w_1 \text{ is not joined by an edge in } P(i,j) \text{ to } v_i, \text{ and } w_{k-1} \text{ is joined by an edge to } v_{i+k}.\}$$

$$W_i^\Gamma(1,1) = \{(w_1, ..., w_{k-1}) : w_1 \text{ is not joined by an edge in } P(i,j) \text{ to } v_i, \text{ and } w_{k-1} \text{ is not joined by an edge to } v_{i+k}.\}$$

Clearly, the set $W_i^\Gamma(0,0)$ counts the number of paths that can be inserted in place of $v_{i+i}, ..., v_{i+k-1}$ to obtain a path in $C^\Gamma(\gamma)$, and $W_i^\Gamma(1,1)$ counts the corresponding figure for $C^{\Gamma^f}(\gamma)$. We will establish the lemma if we can show that the cardinality of $W_i^\Gamma(0,0)$ equals that of $W_i^\Gamma(1,1)$.

But from the regularity of the graphs C_i, it follows that the number of paths $\{(w_1, ..., w_{k-1})\}$ lying in W_i^Γ beginning at a given w_1 is independent of w_1, and is equal to the number of paths $\{(w_1, ..., w_{k-1})\}$ ending at a given w_{k-1}.

It follows that

$$W_i^\Gamma(0,0) + W_i^\Gamma(0,1) = W_i^\Gamma(0,1) + W_i^\Gamma(1,1),$$

from which we see that

$$W_i^{\Gamma}(0, 0) = W_i^{\Gamma}(1, 1).$$

This completes the proof of the lemma.

To establish the theorem, we apply this construction to the case where

$$C_i = C \qquad \text{for} \quad i \neq 0, \quad k-l$$
$$C_0 = \tilde{C}$$
$$C_{k-1} = \tilde{C}',$$

where $\tilde{C}$ is the 4-regular graph obtained from C by attaching a loop to each vertex, and $\tilde{C}'$ is obtained from C by adjoining two edges to each vertex without forming any additional loops.

For all i and j, $P(i, j)$ is empty if $|j-i| \neq 1$, and $P(i, i+1)$ is as in the example.

The lemma now applies to show that for the 2^{k-1} functions

$$f: \{0, ..., k-1\} \to \{0, 1\} \qquad \text{with} \quad f(0) = 0,$$

the graphs Γ^f are mutually isospectral. Furthermore, we may readily reconstruct f from Γ^f as follows: the subgraph $\tilde{C}$ is easily determined by the fact that the only vertices with two loops belong to it. After $\tilde{C}$ is determined, C_1 is determined by the fact that it consists of all vertices joined to $\tilde{C}$ other than the vertices of $\tilde{C}$. We may then check whether $f(1)$ agrees with $f(0)$ by determining whether or not the subgraph with vertices in $\tilde{C}$ and C_1 is planar.

Continuing inductively in this way, we reconstruct f.

This completes the proof of the theorem.

2. ALMOST INNER AUTOMORPHISMS

We begin with the following definition:

DEFINITION 2.1. Let G be a finite group, and H_1 and H_2 two subgroups of G. H_1 and H_2 are *almost conjugate* in G if they satisfy:

(†) for all $g \in G$, $|[g] \cap H_i|$, is independent of i.

Here $[g]$ denotes the conjugacy class of g in G, and $|[g] \cap H_i|$ is the cardinality of $[g] \cap H_i$.

Conjugate subgroups of G are necessarily almost conjugate, but we will be particularly interested in almost conjugate subgroups that are not conjugate.

The interest in almost-conjugate subgroups comes from the following theorem of Sunada:

THEOREM 2.1 ([Su]). *Let G be a finite group, and H_i a family of mutually almost conjugate subgroups of G.*

Let M be a Riemannian manifold, and $\phi: \pi_1(M) \to G$ a homomorphism of the fundamental group of M onto G. For each i, let M^{H_i} be the Riemannian covering of M whose fundamental group is $\phi^{-1}(H_i)$.

Then the manifolds M^{H_i} are mutually isospectral.

Thus, the property of being almost conjugate can be thought of as a translation into group theory of the notion of isospectrality. Note that if H_i is conjugate to H_j, then M^{H_i} is isometric to M^{H_j}.

The remainder of this section, which will be entirely algebraic in character, will be devoted to finding finite groups that have large numbers of mutually almost conjugate subgroups which are not conjugate.

One way to construct almost conjugate subgroups is via *almost inner automorphisms*:

DEFINITION 2.2. An automorphism ϕ of G is said to be *almost inner* if, for all $g \in G$, $\phi(g)$ and g are conjugate in G.

It is evident that if $\phi_1, ..., \phi_k$ are almost inner automorphisms of G, then $H, \phi_1(H), ..., \phi_k(H)$ satisfy (†).

We will approach the problem of finding groups G with large numbers of almost conjugate subgroups in two steps: first, we will find groups G which admit large numbers of almost inner but not inner automorphisms. Then we will find a subgroup H of G such that the orbit of H under the action of these almost inner automorphisms is large.

For R a commutative ring with unity, let $G = G(R)$ denote the three-dimensional Heisenberg group over R, given by

$$G = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in R \right\}.$$

We write an element of G as (x, y, z) in the obvious manner. We then have the multiplication rule

$$(x, y, z) * (x', y', z') = (x + x', y + y', z + z' + xy').$$

Note that $(0, 0, 0)$ is the identity element, while the inverse of (x, y, z) is $(-x, -y, -z+xy)$.

It follows that the conjugates of (x, y, z) are all elements of the form $(x, y, z+ax+by)$. More precisely, (x, y, z) and (x', y', z') are conjugate in G if and only if $x=x'$, $y=y'$, and $z-z' \in Rx+Ry$, where Rx denotes the principal ideal of R generated by x.

Now let $f: R \times R \to R$ be any function.

LEMMA 2.1. *The map* $\psi_f: G \to G$ *given by*

$$\psi_f(x, y, z) = (x, y, z + f(x, y))$$

is an automorphism if and only if f *is an additive group homomorphism.*

Proof. For any mapping f, ψ_f is clearly 1-1 and onto.

In order for ψ_f to be an automorphism, we must have that

$$\psi_f(x, y, z) * \psi_f(x', y', z') = \psi_f(x+x', y+y', z+z'+xy').$$

But it follows directly from the definitions that this is so if and only if $f((x, y)+(x', y')) = f(x, y)+f(x', y')$, as desired. ∎

DEFINITION 2.3. (a) Let R_1 and R_2 be R-modules. A function $f: R_1 \to R_2$ is *R-linear* if f is an additive group homomorphism and $f(rx) = rf(x)$ for all r in R; i.e., f is a homomorphism of R-modules.

(b) Let M be a free R-module with basis $\{m_1, ..., m_k\}$. A function $f: M \to R$ is *almost linear* if f is an additive group homomorphism and $f(\sum r_i m_i) \in \sum Rr_i$ for all r_i in R.

We observe that the condition in (b) above is independent of the choice of basis $\{m_1, ..., m_k\}$.

Roughly speaking, an almost-linear function $f: R \times R \to R$ is a function satisfying

$$f(x, y) = a(x)\, x + b(y)\, y,$$

where the coefficients $a(x)$ and $b(y)$ need not be constant, but which satisfy the "almost-constant" condition

$$a(x_1+x_2)(x_1+x_2) = a(x_1)\, x_1 + a(x_2)\, x_2$$

$$b(y_1+y_2)(y_1+y_2) = b(y_1)\, y_1 + b(y_2)\, y_2.$$

We now have:

LEMMA 2.2. (a) *ψ_f is inner if and only if f is R-linear.*

(b) *ψ_f is almost inner if and only if f is almost linear.*

Proof. (b) is just rewriting the fact that $(x, y, z + f(x, y))$ is conjugate to (x, y, z) if and only if $f(x, y)$ can be written in the form $f(x, y) = ax + by$. To show (a), it suffices to check that

$$(f(0, 1), -f(1, 0), 0)$$

conjugates (x, y, z) to $(x, y, z + f(x, y))$ in the case where f is R-linear. ∎

Let us denote by $AL = AL(R \times R, R)$ the space of almost linear functions, and $L(R \times R, R)$ the R-linear functions. If we denote by AI the almost inner automorphisms of G and by I the inner automorphisms, then by Lemma 2.2, we may identify AI/I with AL/L.

EXAMPLE 2.1. Let $R = \mathbb{F}_{p^n}$, the unique field with p^n elements. The field $\mathbb{F}_{p^n}$ is a field extension of $\mathbb{F}_p$ of degree n, hence an n-dimensional $\mathbb{F}_p$-vector space. Here $AL(R \times R, R)$ is precisely the set of $\mathbb{F}_p$-linear maps. Indeed, the condition that f is an additive group homomorphism implies that it is $\mathbb{F}_p$-linear, and the condition that $f(x, y) \in Rx + Ry$ is automatically satisfied if $f(0, 0) = 0$, since a field has no ideals other than itself and (0).

Thus AL is a vector space of dimension $2n^2$ over $\mathbb{F}_p$, while L has dimension 2 over $\mathbb{F}_{p^n}$, and hence dimension $2n$ over $\mathbb{F}_p$. As $\mathbb{F}_p$ has order p, it follows that

$$|AI/I| = p^{2n(n-1)}.$$

EXAMPLE 2.2. Let $R = \mathbb{F}_p \times \mathbb{F}_p \times \cdots \times \mathbb{F}_p$. Again, f an additive group homomorphism implies that it is $\mathbb{F}_p$-linear. However, if we set e_i to be the element of R which has i-coordinate equal to 1 and all other coordinates 0, then the almost linearity condition gives us that

$$f(e_i, 0) = a_i \cdot e_i$$

and

$$f(0, e_i) = b_i \cdot e_i$$

for some a_i and b_i.

If we now set a to be the element of R that agrees with a_i in the ith place for all i, and the same for b, then we have that

$$f(x, y) = ax + by$$

for all x, y in R, so that f is in fact linear.

It follows that $|AL/L| = |AI/I| = 1$ in this case.

EXAMPLE 2.3. Let $R = \mathbb{F}_p[x]/(x^n)$.

The condition that f be an additive group homomorphism is again that f is $\mathbb{F}_p$-linear. Thus, f is determined by the values $f(x^i, 0)$ and $f(0, x^j)$, $i, j = 0, 1, ..., n-1$.

The almost linear condition is then that

$$f(x^i, 0) \in Rx^i, \qquad f(0, x^j) \in Rx^j.$$

We see immediately from this that

$$\dim_{\mathbb{F}_p}(AL(R \times R, R)) = 2[n + (n-1) + \cdots + 1] = n^2 + n.$$

On the other hand, $\dim_{\mathbb{F}_p}(L(R \times R, R)) = 2n$, so that we have

$$|AI/I| = p^{n(n-1)}.$$

We now turn to the problem of the orbit of a subgroup H under almost-inner automorphisms.

Let H be the subgroup of G given by

$$H = \left\{ \begin{pmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : x \in R \right\}.$$

Note that $|H| = |R|$. If f is almost linear, we have

$$\psi_f(H) = \left\{ \begin{pmatrix} 1 & x & f(x, 0) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : x \in R \right\}.$$

Define $H_f = \psi_f(H)$. Clearly, we can reconstruct $f(x, 0)$ from H_f, so that

$$H_f = H_{f'} \quad \text{if and only if} \quad f(x, 0) = f'(x, 0) \quad \text{for all} \quad x \in R.$$

If we set $\bar{f} = f(x, 0)$, we easily check that $\bar{f}$ is R-linear (resp. almost linear) if f is R-linear (resp. almost linear).

Note that H and H_f are almost conjugate in G if and only if $\bar{f}$ is almost linear, and H and H_f are conjugate if and only if $\bar{f}$ is R-linear. It follows that the set $AC(H)$ of H_f's modulo equivalence by inner automorphisms is given by

$$AC(H) \cong AL(R, R)/L(R, R).$$

EXAMPLE 2.1, CONTINUED. When $R = \mathbb{F}_{p^n}$, we have that

$$|AL(R, R)| = p^{n^2} \qquad \text{and} \qquad |L(R, R)| = p^n,$$

so that the number of almost conjugate, nonconjugate H_f's is given by

$$|AC(H)| = p^{n(n-1)}.$$

EXAMPLE 2.3, CONTINUED. Similarly, for $R = \mathbb{F}_p[x]/(x^n)$, we have that

$$|AL(R)| = p^{n(n+1)/2} \qquad \text{and} \qquad |L(R, R)| = p^n,$$

so that the number of almost conjugate, nonconjugate H_f's is given by

$$|AC(H)| = p^{n(n+1)/2}.$$

3. RIEMANN SURFACES

In this section, we will complete the proof of Theorem 0.3.

In light of the Sunada Theorem 2.1 and the construction of Section 2, it suffices to consider homomorphisms

$$\phi: \pi_1(S) \to G(R)$$

for various choices of R. We will want to choose the genus of S small, and will have to verify that the large number of isospectral surfaces constructed are indeed distinct Riemann surfaces.

As in Section 2, let $G = G(R)$ denote the Heisenberg group over the ring R, and let H be the subgroup

$$H = \left\{ \begin{pmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : x \in R \right\}.$$

For convenience, we assume that R is a finite-dimensional $\mathbb{F}_p$-algebra. Denote by n the $\mathbb{F}_p$-dimension of the additive group of R.

Suppose we have a surface S with an onto homomorphism $\mu: \pi_1(S) \to G$. If g_0 denotes the genus of S, then according to the Sunada Theorem 2.1, the surfaces S^{H_f} are mutually isospectral. Since these surfaces are all coverings of S of degree $|G/H| = |R^2|$, and since $g - 1$ is multiplicative under coverings, we have that

$$g(S^{H_f}) = 1 + |G/H|\,(g_0 - 1) = 1 + |R|^2\,(g_0 - 1).$$

We now want to choose S so that g_0 is as small as possible, but so that all the surfaces S^{H_f} are distinct; i.e. nonisometric.

We first observe that an onto homomorphism $\mu: \pi_1(S) \to G$ induces an onto homomorphism $H_1(S) \to G/[G, G] \cong R \times R$, where $H_1(S)$ denotes the first homology group of S, and has rank $2g_0$. Since this last has rank $2n$, we see that g_0 must be at least n.

We now claim that G can be generated by $2n$ generators. If $1 = \zeta_1, ..., \zeta_n$ denotes a basis for the additive group of R, then we have:

LEMMA 3.1. *G is generated by the set X consisting of the $2n$ elements*

$$X = \{(\zeta_1, 0, 0), ..., (\zeta_n, 0, 0), (0, \zeta_1, 0)..., (0, \zeta_n, 0)\}.$$

Proof. We have that

$$(-\zeta_i, 0, 0) * (0, -\zeta_j, 0) * (\zeta_i, 0, 0) * (0, -\zeta_j, 0) = (0, 0, \zeta_i, \zeta_j).$$

Taking $i = 1$ and j arbitrary shows that all the elementss $(0, 0, z)$ lie in the subgroup generated by X. It is clear that the subgroup generated by X contains all elements of the form $(x, 0, 0)$ and $(0, y, 0)$. Writing a general element as

$$(x, y, z) = (0, y, 0) * (x, 0, 0) * (0, 0, z)$$

completes the argument. ∎

We now claim:

LEMMA 3.2. *There is an onto homomorphism $\mu: \pi_1(S) \to G$ with*

$$g(S) = n \qquad \text{if } n \text{ is even}$$
$$g(S) = n + 1 \qquad \text{if } n \text{ is odd}$$

Proof. We recall that if $g(S) = k$, then $\pi_1(S)$ has the presentation

$$\pi_1(S) = \{A_1, B_1, ..., A_k, B_k : \Pi_k[A_i, B_i] = 1\}.$$

To construct a homomorphism of $\pi_1(S)$, we need only check that the relation is satisfied in the image.

When n is even, we may choose $k = n$, and send $A_1, B_1, ..., A_{n/2}, B_{n/2}$ arbitrarily to the set of generators $(\zeta_n, 0, 0), ..., (\zeta_n, 0, 0)$, and $A_{(n/2)+1}, B_{(n/2)+1}, ..., A_n, B_n$ arbitrarily to $(0, \zeta_1, 0), ..., (0, \zeta_n, 0)$. The relation is clearly satisfied because all the commutators involved are 0.

When n is odd, we may choose $k = n + 1$ and send $A_1, B_1, ..., A_{(n+1)/2)}, B_{(n+1)/2)}$ arbitrarily onto $(\zeta_1, 0, 0), ..., (\zeta_n, 0, 0)$ (one generator will be hit

twice), and similarly for $A_{(n+1)/2+1}, B_{(n+1)/2+1}, \ldots, A_n, B_n$. The relation is again satisfied, for the same reason. ∎

In the case of Example 2.1, when $R = \mathbb{F}_{p^n}$, we can do better:

LEMMA 3.3. *There is an onto homomorphism* $\mu: \pi_1(S) \to G(\mathbb{F}_{p^n})$ *with* $g(S) = n$.

Proof. In the case n even, this was shown in Lemma 3.2.

In the case when n need not be even, we may proceed as follows:

Since the multiplicative group of $\mathbb{F}_{p^n}$ is cyclic, we can choose ζ a generator of the multiplicative group. We then have that $1, \zeta, \ldots, \zeta^{(n-1)}$ generate $\mathbb{F}_{p^n}$ as a vector space over $\mathbb{F}_p$.

Let us set

$$C = \sum_{i=0}^{n-1} \zeta^{2i} = \sum_{i=0}^{n-1} c_i \zeta^i.$$

and write

$$\zeta^n = \sum_{i=0}^{n-1} b_i \zeta^i.$$

We will need the fact that $b_0 \neq 0$. This follows from the fact that ζ satisfies an irreducible polynomial of degree n. If the constant term were 0, the polynomial would not be irreducible.

We now consider the homomorphism $v: \pi_1(S) \to G$ given by:

$$v(A_1) = \left(1 + \sum_{i=1}^{n-1} a_i \zeta^i, 0, 0\right)$$

$$v(A_i) = (\zeta^{i-1}, 0, 0) \qquad \text{for} \quad i \neq 1$$

$$v(B_2) = (0, \zeta - b\zeta^{n-1}, 0)$$

$$v(B_i) = (0, \zeta^{i-1}, 0) \qquad \text{for} \quad i \neq 2.$$

Since we have set $a_0 = 0$, it is clear that the image generates G.

We now compute:

$$v(\Pi[A_i, B_i]) = C - b\zeta^n + \sum_{i=1}^{n-1} a_i \zeta^i = \left(\sum_{i=1}^{n-1} c_i - bb_i\right) + \sum_{i=1}^{n-1} a_i \zeta^i.$$

Since $b_0 \neq 0$, we may choose $b = c_0/b_0$ and then $a_i = bb_i - c_i$ to obtain

$$v(\Pi[A_i, B_i]) = 0.$$

This completes the proof of the lemma. ∎

Using this choice of generators, we have constructed $p^{(n^2-n)}$ surfaces of genus $1 + (n-1)\, p^{2n}$. We must now show that they are pairwise distinct. This is made possible by the following theorems of Greenberg and Margulis, as described in [Su]:

THEOREM 3.1 ([Gr]). *For a generic Riemann surface $S = \mathbb{H}/\Gamma$ of genus $g > 2$, Γ is not contained in any larger discrete subgroup of $PSL(2, \mathbb{R})$.*

Here, $\mathbb{H}$ denotes the hyperbolic plane.

THEOREM 3.2 ([M]). *If Γ is not an arithmetic group, the commensurator group of Γ is discrete.*

Recall that the commensurator group $C(\Gamma)$ of F is the set of all isometries g of $\mathbb{H}$ such that $g\Gamma g^{-1}$ intersects Γ in a subgroup of finite index. Clearly, $C(\Gamma)$ contains Γ. The two theorems above taken together tell us that for a generic non-arithmetic Γ with the genus of $\mathbb{H}/\Gamma > 2$, $C(\Gamma)$ is equal to Γ.

Now suppose that $S^{H_{f_1}}$ is isometric to $S^{H_{f_2}}$. Then this isometry lifts to an isometry of $\mathbb{H}$ to itself, which takes $\mu^{-1}(H_{f_1})$ to $\mu^{-1}(H_{f_2})$, and hence lies in the commensurator subgroup of Γ. But the commensurator group condition insures that it must be an element of Γ. Pushing this forward by μ, we then have an element of G which conjugates H_{f_1} to H_{f_2}. This contradicts the fact that H_{f_1} and H_{f_2} are not conjugate in G.

Picking S to be one of these generic surfaces completes the argument. ∎

This now completes the proof of Theorem 0.3. We remark that the evaluation of the constant $c = 1/(4\log(2))$ follows by taking $p = 2$ and sending $n \to \infty$.

Remark. We remark that analogous constructions based on more general Heisenberg-type groups also yield families of mutually isospectral surfaces growing at approximately the same rate as the present examples. However, the constants involved are worse than in the present examples. In addition, constructions based on higher-step nilpotent Lie groups are considerably more rigid, and do not yield families of comparable size.

We plan to examine the algebra of these more elaborate examples elsewhere.

4. NUMBER FIELDS

In this section, we prove Theorem 0.5.

The following appears as an exercise in [CF]:

THEOREM 4.1. *Let G be the Galois group of a number field K over $\mathbb{Q}$, and let H_1 and H_2 be two subgroups of G satisfying* (†).

If K^{H_1} and K^{H_2} denote the fixed fields of H_1 and H_2 respectively, then the zeta functions $\zeta_{K^{H_1}}(S)$ and $\zeta_{K^{H_2}}(S)$ are equal.

According to [Per], all pairs of number fields whose zeta functions are equal arise in this manner.

Theorem 0.5 follows immediately from this together with the construction of Section 2, once we know that the groups $G(\mathbb{F}_{p^n})$ arise as Galois groups of a number field over $\mathbb{Q}$. However, it follows from a theorem of Reichardt [Re] that, for $p \neq 2$, all p-groups are realized as Galois groups over $\mathbb{Q}$. The case $p = 2$ was given incorrect proofs and then corrected by Shafarevich. See [Se] for a discussion of the history of this result.

ACKNOWLEDGMENTS

R. Brooks and R. Gornet extend their thanks to the joint NSF-CNRS program in Spectral Geometry for their support of the workshop in Dartmouth in February, 1996, where much of this work was carried out. R. Brooks also thanks the Department of Mathematics at Texas Tech University for their support of this area of research. R. Brooks was partially supported by a Guastella Fellowship, the Fund for the Promotion of Research at the Technion, and the M. and M. L. Bank Mathematics Research Fund. R. Gornet was partially supported by the Texas Advanced Research Program under Grant No. 003644–002.

REFERENCES

[BL] R. Brooks and A. Lubotzky, Non sunada graphs, in preparation.

[Bu] P. Buser, "Geometry and Spectra of Compact Riemann Surfaces," Basel, 1992.

[CF] J. W. S. Cassels and A. Fröhlich (Eds.), "Algebraic Number Theory," Academic Press, San Diego, 1967.

[CDGT] D. Cvetković, M. Doob, I. Gutman, and A. Torgasev, "Recent Results in the Theory of the Graph Spectra," Amsterdam, North-Holland, 1988.

[DG] D. DeTurck and C. S. Gordon, Isospectral deformations. I. Riemannian structures on two-step nilspaces, *Comm. Pure Math.* **40** (1988), 367–387.

[GW] C. S. Gordon and E. Wilson, Isospectral deformations of compact solvmanifolds, *J. Differential Geom.* **19** (1984), 241–256.

[Gr] L. Greenberg, Maximal fuchsian groups, *Bull. Amer. Math. Soc.* **69** (1963), 569–573.

[M] G. Margulis, Discrete groups of motions of manifolds of non-positive curvature, *in* "Proceedings International Congress, Vancouver, 1974," Vol. 2, pp. 21–34. [In Russian].

[Per] R. Perlis, On the equation $\zeta_K(s) = \zeta_{K'}(s)$, *J. Number Theory* **9** (1977), 342–360.

[Re] H. Reichardt, Konstruktion von Zahlkoerpern mit gegebener Galoisgruppe von Primzahlpotentzordnung, *J. Reine Angew. Math.* **177** (1937), 1–5.

[Se] J. P. Serre, "Topics in Galois Theory," Jones and Bartlett, Boston, 1992.

[Su] T. Sunada, Riemannian coverings and isospectral manifolds, *Ann. of Math.* **121** (1985), 169–186.

[Tse1] R. Tse, "A Lower Bound for the Number of Isospectral Surfaces of Arbitrarily Large Genus," Ph.D. thesis, University of Southern California, 1988.

[Tse2] R. Tse, A lower bound for the number of isospectral surfaces, *in* "Recent Developments in Geometry" (Cheng, Choi, and Greene, Eds.), *Contemp. Math.* **101** (1989), 161–164.

[Vig1] M. F. Vignéras, Exemples de sous-groupes discretes non-conjugués de $PSL(2, \mathbb{R})$ qui ont même fonction zêta de Selberg, *C. R. Acad. Sci. Paris* **287** (1978), 47–49.

[Vig2] M. F. Vignéras, Variétés Riemanniennes Isospectrales et non Isométriques, *Ann. of Math.* **112** (1980), 21–32.